REMARKS

The Office Action dated July 19, 2004 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claim 15 has been amended. No new matter has been added. Claims 7-9 and 11-33 are respectfully submitted for consideration.

Claims 7, 21-26 and 30 were objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claims 8, 9, 11, 13 - 20, 27, 28 and 29 were rejected under 35 USC § 103(a) as being unpatentable over U.S. Patent No. 6,400,707 to Baum et al. in view of U.S. Patent No. 6,233,234 to Curry et al. The rejection is traversed as being based on references that neither teach nor suggest the novel combination of features clearly recited in independent claims 11, 15 and 20.

Claim 11, upon which claims 7-9 and 12-14 are dependent, recites a method for switching VOIP packets in a data network. The method includes the steps of receiving a first packet in a network switch and determining if the first packet is a VOIP packet. The method also includes the step of determining a dynamically negotiated VOIP port for a VOIP session from at least one of the first packet and a second packet received in the network switch, if the first packet is determined to be the VOIP packet. The method further includes the step of classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters. The step of classifying all subsequent VOIP packets further includes storing the dynamically negotiated VOIP port, filtering all packets coming through the network switch having the dynamically negotiated VOIP port associated therewith and classifying filtered packets in accordance with predefined filtering actions. The step of storing the dynamically negotiated VOIP port further includes generating a filter corresponding to the dynamically negotiated VOIP port and storing the generated filter in a filter table associated with a fast filtering processor.

Claim 15, upon which claims 16-19 depend, recites a method for switching VOIP packets. The method includes the steps of filtering packets received in a network switch to trap at least one VOIP call setup message and determining a dynamically negotiated VOIP port. The method also includes the steps of filtering all subsequent packets associated with the dynamically negotiated VOIP port and taking predefined filtering actions upon the subsequent packets. The steps of filtering packets and determining the dynamically negotiated VOIP port further includes generating a filter corresponding to the dynamically negotiated VOIP port and storing the generated filter in a filter table associated with a fast filtering processor.

Claim 20, upon which claims 21-30 are dependent, recites a network switch for switching VOIP packets. The network switch includes at least one data port interface controller supporting a plurality of data ports for transmitting and receiving data and a fast filtering processor in communication with the at least one data port interface. The network switch also includes at least one filtering table in communication with the fast filtering processor. The fast filtering processor is configured to snoop packets being transmitted through the network switch to trap a VOIP call setup message, and thereafter, determine a dynamically negotiated VOIP port so that all subsequent VOIP packets can be filtered and assigned an appropriate priority.

As will be discussed below, the cited prior art references of Baum et al. and Curry et al. fail to disclose or suggest the elements of any of the presently pending claims.

Baum et al. teaches a method for managing security in communication session across a hybrid network. Col. 1, lines 4-12. According to figure 1 of Baum et al., the network includes a packet switched network and a circuit switched network, a directory, an authentication and security accounting object and an Internet Telephony Gateway. The directory matches called party exchange numbers to IP addresses of gateways which serve the respective exchange numbers. The authentication and security accounting object performs customer authentication, call authorization, usage accounting and usage pricing. The Internet Telephony Gateway connects the packet switched and circuit switched networks. Call setup starts when a user establishes IP layer connectivity with the network. Thereafter, the user launches a VOIP application and populates a telephone number to be called in a data field. Col. 3, line 40 – Col. 4, line 14. The user initiates the call via the VOIP application, which invokes the directory to obtain the IP address of the destination gateway. The VOIP application invokes the gateway to setup the call by passing to the gateway the number to be called, the user account number and password.

The gateway then invokes the authentication database to receive authorization to proceed with the call. If authorization was successful, the gateway establishes the PSTN connection and notifies the client software that the call is proceeding. Col. 4, lines 15 – 63.

Figure 3 of Baum et al. shows a detailed depiction of the network with a firewall mechanism. According to figure 3, the IP network is connected to a switched telephone network through gateways. The IP network is connected to the gateways through a firewall mechanism that includes a static firewall router, a hub packet switch and a control processor. The static firewall router acts as a rule based packet filter. The rules are automatically and dynamically set. The security is applied to each port on the fly to provide extremely fast operation. Baum et al. teaches the generation and application of customized filters for each conversation, wherein each filter is unique to a specific conversation and disappears on the termination of the conversation. As a result, a high level of security is obtained. The static firewall router copies the signaling which occurs during setup of a communication path and delivers the two data streams to the packet switch which passes the original stream to the addressed gateway and the copied stream to the control processor. The control processor monitors and analyzes the setup signaling which follows and derives critical parameters which are used to govern the ensuing conversation. The control processor then compiles a filter code from the parameters and sends the filter code to the firewall. Col. 5, line 24 – Col. 6, line 32.

According to figures 3 and 4 of Baum, the PC initiates the call via the VOIP application and is authenticated and registered through the authorization platform. The directory is accessed to obtain the IP address of the destination gateway. The PC notes the address of the gateway and uses it to send a Q.931 message to setup a conversation. The message reaches the static firewall which has only one port open for Q.931 messages. If the message is a valid Q.931 stream and includes the Q.931 port address in the firewall and the IP address of the gateway, the firewall commences replication of the signaling stream and passes both streams to the packet switch. The packet switch sends to original stream to the gateway and the copied stream to the control processor. The control processor analyzes the replicated stream and notes that it has a request, where it originated and that it is an H.232 over Q.931 set up signal. The gateway verifies that it has a valid customer and sends a negotiation message, with a proposal of the gateway for a codec and port, back to the PC. The negotiation message passes through the firewall which copies the message and sends the copy to the control processor. The control processor reads and analyzes the replicated message, notes the codec and port and notes that the gateway has authorized the call. An acceptance message is received by the gateway and the gateway returns an acknowledgement to the call via the switch and the firewall. This message is copied by the firewall and sent to the control processor which registers that a valid conversation as been established on a designated port. The control processor then generates a set of security specifications, compiles a filter configuration message and sends the message to the firewall. The firewall sets up a very specific filter for this single conversation. The firewall now monitors every packet that follows for conformance with the filter requirements. The control processor drops out and turns to other set-ups. Col. 6, line 36 – Col. 9, line 19.

Curry et al teaches providing telephony communication through a packet switched data network and on organization having a telephone and computer terminals connected to a LAN. To address security issues associated with TCP/IP protocol, Curry et al. relies on a hardware address filter table. The address filter table may be applied to both incoming and outgoing addresses. Col. 5, line 64 - Col. 6, line 28.

Applicants respectfully submit that the combination of Baum et al. and Curry et al. fails to teach or suggest the combination of elements recited in claims 11, 15 and 20. Claim 11, in part, recites classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters; wherein the step of classifying all subsequent VOIP packets further comprises, storing the dynamically negotiated VOIP port; filtering all packets coming through the network switch having the dynamically negotiated VOIP port associated therewith; and classifying filtered packets in accordance with predefined filtering actions; and wherein the step of storing the dynamically negotiated VOIP port further comprises generating a filter corresponding to the dynamically negotiated VOIP port and storing the generated filter in a filter table associated with a fast filtering processor. Claim 15, in part, recites classifying all subsequent packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters and taking predefined filtering actions upon the subsequent packets. Claim 20, in part, recites the fast filtering processor is configured to snoop packets being transmitted through the network switch to trap a VOIP call setup message, and thereafter, determine a dynamically negotiated VOIP port so that all subsequent VOIP packets can be filtered and assigned an appropriate priority. Applicants submit that Baum et al. does not teach or suggest classifying or assigning priority to all subsequent packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters as recited in claims 11, 15 and 20. According to Baum et al., the firewall filter monitors every packet that follows after the setup messages for conformance with the strict filter requirements. There is simply no discussion or suggestion in Baum et al. of classification of all subsequent packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters as recited in claims 11, 15 and 20.

Curry et al. fails to cure the deficiencies of Baum et al. as Curry et al. also does not discuss or suggest classifying or assigning priority to all subsequent packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters as recited in claims 11, 15 and 20. Therefore, Applicants respectfully assert that the rejection under 35 U.S.C. §103(a) should be withdrawn because neither Baum et al. nor Curry et al., whether taken singly or combined, teaches or suggests each feature of claims 11, 15 and 20 and hence, dependent claims 8, 9, 13, 14, 16-19, 27, 28 and 29 thereon.

Claims 12, 31 and 32 were rejected under 35 U.S.C. 103(a) as being unpatentbale over Baum et al. in view of Curry et al., further in view of U.S. Patent No. 6,085328 to Klein et al. The rejection is traversed as being based on references that neither teach nor suggest the novel combination of features clearly recited in independent claims 11, upon which claim 12 is dependent, 31 and 32.

Claim 31 recites a method for switching VOIP packets in a data network. The method includes the steps of receiving a first packet in a network switch, determining if the first packet is a VOIP packet, determining a dynamically negotiated VOIP port for a VOIP session from at least one of the first packet and a second packet received in the network switch, if the first packet is determined to be the VOIP packet and classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters. The steps of determining if the first packet is a VOIP packet, determining a dynamically negotiated VOIP port, and classifying subsequent VOIP packets are performed in a filtering step by a fast filtering processor. Additionally, the filtering step further includes applying a filter mask to a header of a packet, extracting unmasked information, comparing the unmasked information to a filtering table and executing predetermined filtering actions based upon the comparison to the filtering table.

Claim 32, from which claim 33 depends, recites a method for switching VOIP packets in a data network. The method includes the steps of receiving a first packet in a network switch, determining if the first packet is a VOIP packet, determining a dynamically negotiated VOIP port for a VOIP session from at least one of the first packet and a second packet received in the network switch, if the first packet is determined to be the VOIP packet and classifying all subsequent VOIP packets corresponding to the dynamically negotiated VOIP port in accordance with predetermined parameters. The step of determining if the first packet is a VOIP packet further includes the steps of applying a filter mask to the packet header, comparing unmasked information from the header to entries in a filter table to determine a match and determining if a VOIP well known port is contained in the packet header.

Applicants respectfully assert that even with the addition of the teachings of Klein et al., the deficiencies of Baum et al. and Curry et al. are not cured. Klein et al. is directed to a method of waking up a sleeping computer using packet snooping and imperfect filtering. The Office Action highlights Fig. 4 of Klein et al., and its associated discussion, as teaching the application of a mask to a packet and a hash function is calculated. The result is used in a decision process to compare the resulting 16 bit value with certain values to determine whether the computer should be awakened.

First, it is noted Klein et al. fails to teach or suggest the elements, discussed above, that are not taught or suggested by Baum et al. and Curry et al. Klein et al. also fails to disclose extracting unmasked information and comparing the unmasked information to a filtering table as recited in claims 12, 31 and 32. Instead Klein et al. teaches that at block 412, a mask is selected for hash function calculation and the selected mask is tested at decision block 414. If a match does not occur, decision blocks 416-420 are implemented until all masks have been tested. There is simply no teaching or suggestion in Klein et al. of extracting unmasked information and comparing the unmasked information to a filtering table. Thus, Applicants respectfully assert that that for these reasons, claims 12, 31 and 32 should be allowed over Baum et al., Curry et al. and Klein et al.

In view of the above, Applicants respectfully submit that independent claims 11, 15, 20, 31 and 32 each recite subject matter which is neither disclosed nor suggested in a combination of Baum et al. , Curry et al. and Klein et al. In addition, claims 7-9, 12-14, 16-19, 21-30 and 33, depend from the independent claims and should likewise be allowed for at least their dependence on the independent claims. It is therefore respectfully requested that all of claims 7-9 and 11-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the Applicants' undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Arlene P. Neal

Arlene P. Neal
Registration No. 43,828

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802